IN THE CLAIMS:

This listing of claims will replace all prior versions and listings, of claims in the

application:

Listing of Claims:

1-8. (Cancelled)

9. (Currently Amended) A system, comprising:

at least one personal computer, said personal computer configured to operate with at least

one other computer connected to a network;

said personal computer including at least one microchip having at least one microprocessor

with at least one control unit and at least two processing units, said control unit including means

for at least one user of said personal computer to control said at least two processing units, and said

microchip including at least one power management component;

said personal computer including at least one internal firewall, said internal firewall

~~capable of allowing and/or denying~~ configured to allow and/or deny access to portions of said

microchip both to at least one user of said personal computer and to at least one user of said

microchip from said network during shared use of said microchip; and said internal firewall being

configured to deny access to portions of said microchip from said network.

10. (Previously Presented) The system of claim 9, wherein said personal computer

includes at least one camera component.

11. (Cancelled)

12.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one videocam component.

13.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one radio component.

14.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one television component.

15.   (Previously Presented)   The system of claim 9, wherein said personal computer includes Flash memory.

16.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one hard drive.

17.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one digital signal processor.

18.   (Previously Presented)   The system of claim 9, wherein said network includes a World Wide Web which is utilized to provide shared computer processing resources.

19.   (Cancelled)

20.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one direct optical fiber network connection.

21.   (Cancelled)

22.   (Previously Presented)   The system of claim 9, wherein said personal computer includes at least one direct wireless connection from said personal computer to said other computer connected to said network.

23.   (Cancelled)

24.   (Cancelled)

25. (Previously Presented) The system of claim 9, wherein said personal computer is equipment of an automobile or other transportation vehicle or other conveyance .

26. (Previously Presented) The system of claim 9, wherein said microchip includes:

at least one digital signal processor; or

at least one network communications component; or

both.

27. (Previously Presented) The system of claim 9, further comprising a shared processing operation, which includes:

parallel processing; or

multi-processing; or

multi-tasking; or

any combination thereof.

28. (Cancelled)

29. (Cancelled)

30. (Previously Presented) The system of claim 9, wherein said personal computer is configured so that at least one user of said personal computer retains preemptive control of all components of said personal computer.

31. (Previously Presented) The system of claim 9, wherein said microchip includes at

least:

four processing units; or

eight processing units; or

16 processing units; or

32 processing units; or

64 processing units; or

128 processing units; or

256 processing units; or

512 processing units; or

1024 processing units.

32. (Previously Presented) The system of claim 9, wherein said personal computer

includes random access memory (RAM), said RAM being located on said microchip.

33. (Previously Presented) The system of claim 9, said microchip includes:

at least one graphics component; or

at least one audio component; or

at least one video processing component; or

at least one flash BIOS; or

any combination thereof.

34. (Previously Presented) The system of claim 11, wherein said personal computer is

configured to operate wirelessly with other said personal computers in a client/server or a peer-to-

peer network architecture.

35. (Previously Presented) The system of claim 9, wherein said at least one microprocessor of said personal computer is controlled by at least one user of said at least one personal computer through said user's operation of at least one wireless controller.

36. (Currently Amended) The system of claim 9, wherein said microchip has at least one internal firewall ~~capable of allowing and denying~~ configured to allow and/or deny access to portions of said microchip both to said user of said personal computer and to users from said network.

37. (Previously Presented) The system of claim 9, wherein:

said internal firewall is configured to deny access to at least said microchip microprocessor control unit of said personal computer by at least one other computer during a shared operation involving said personal computer and said at least one other computer of said network; and

said internal firewall is further configured to allow access to at least one said microchip microprocessor processing unit of said at least one personal computer by at least one of said other computers of said network during said shared operation.

38. (Previously Presented) The system of claim 37, wherein said internal firewall is configured to deny access to at least said microchip microprocessor control unit of said personal computer by said other computers of said network during a shared operation involving said personal computer and at least one of said other computers of said network.

39. (Previously Presented) The system of claim 37, wherein said internal firewall is configured to allow access to at least one said microchip microprocessor processing unit of said personal computer by said other computers of said network during said shared operation.

40. (Previously Presented) The system of claim 39, wherein said internal firewall is configured to deny access to at least one said microchip microprocessor processing unit of said personal computer by at least one user of said personal computer during said shared operation.

41. (Previously Presented) The system of claim 38, wherein said internal firewall is a hardware firewall, a software firewall, a firmware firewall, or another component firewall, or any combination thereof.

42. (Currently Amended) A system, comprising:

at least one personal computer, said personal computer ~~capable of being~~ configured to be directly coupled to another personal computer and/or a server computer by the network;

said personal computer including at least one microchip having at least one microprocessor with at least one control unit and at least two processing units, said control unit including means for at least one user of said personal computer to control the at least two processing units;

said personal computer including at least one internal firewall ~~capable of allowing and/or denying~~ configured to allow and/or deny access to portions of said microchip both to at least one user of said personal computer and to at least one user of said microchip from said network during shared use of said microchip; wherein said internal firewall is a hardware firewall; and

said internal firewall being configured to deny access to portions of said microchip from said network.

43-52. (Cancelled)

53. (Previously Presented) The system of claim 42, wherein said personal computer includes at least one direct optical fiber network connection.

54. (Cancelled)

55. (Previously Presented) The system of claim 42, wherein said personal computer includes at least one wireless connection from said personal computer to said network.

56. (Previously Presented) The system of claim 42, wherein said personal computer is equipment of an automobile or other transportation vehicle or other conveyance.

57. (Previously Presented) The system of claim 42, wherein said microchip includes:

at least one digital signal processor; or

at least one network communications component; or

both.

58-60. (Cancelled) .

61. (Previously Presented) The system of claim 42, wherein said personal computer is configured so that at least one user of said personal computer retains preemptive control of all components of said personal computer.

62. (Previously Presented) The system of claim 42, wherein said microchip includes at least:

four processing units; or

eight processing units; or

16 processing units; or

32 processing units; or

64 processing units; or

128 processing units; or

256 processing units; or

512 processing units; or

1024 processing units.

63. (Previously Presented) The system of claim 42, wherein said personal computer includes random access memory (RAM), said RAM being located on said microchip.

64. (Previously Presented) The system of claim 42, wherein said microchip includes:

at least one graphics component; or

at least one audio component; or

at least one video processing component; or

at least one flash BIOS component; or

any combination thereof.

65. (Cancelled)

66. (Previously Presented) The system of claim 42, wherein said at least one microprocessor of said personal computer is controlled by at least one user of said at least one personal computer through said user's operation of at least one wireless controller.

67. (Currently Amended) The system of claim 42, wherein said microchip has at least one internal firewall ~~capable of allowing and denying~~ configured to allow and deny access to portions of said microchip both to said user of said personal computer and to users from said network.

68. (Previously Presented) The system of claim 42, wherein:

said internal firewall is further configured to deny access to at least said microchip microprocessor control unit of said personal computer by at least one other computer during a shared operation involving said personal computer and said at least one other computers of said network; and

said internal firewall is further configured to allow access to at least one said microchip microprocessor processing unit of said personal computer by at least one of said other computers of said personal network system during said shared operation.

69. (Previously Presented) The system of claim 68, wherein said internal firewall is configured to deny access to at least said microchip microprocessor control unit of said personal computer by said other computers of said personal network system during a shared operation involving said personal computer and at least one of said other computers of said personal network system.

70. (Previously Presented) The system of claim 68, wherein said internal firewall is configured to allow access to at least one said microchip microprocessor processing unit of said personal computer by said other computers of said personal network system during said shared operation.

71. (Previously Presented) The system of claim 70, wherein said internal firewall is configured to deny access to at least one said microchip microprocessor processing unit of said personal computer by at least one user of said personal computer during said shared operation.

72. (Previously Presented) The system of claim 71, wherein said firewall includes hardware or software or firmware or any combination thereof.

73. (Currently Amended) The system of claim 42, wherein said personal computer includes at least one peer to peer wireless network connection ~~capable of coupling~~ configured to couple said personal computer to at least one other personal computer via the wireless network connection.

74. (Currently Amended) A system, comprising:

at least one server computer configured to operate with at least one other computer connected by a network;

said server computer including at least one microchip having at least one microprocessor with at least one control unit and at least two or four or eight or 16 or 32 or 64 or 128 or 256 or 512

or 1024 processing units, said control unit including means for at least one user of a server computer to control said processing units, said microchip including at least one power management component;

and said server computer including at least one internal firewall, said internal firewall ~~capable of allowing and/or denying~~ configured to allow and/or deny access to portions of said microchip both to a user of said server computer and to a user of said microchip from said network during shared use of said microchip; and said internal firewall being configured to deny access to portions of said microchip from said network.

75. (Previously Presented) The system of Claim 9, wherein the internal firewall encloses only a portion of the resources of said personal computer.

76. (Previously Presented) The system of Claim 42, wherein the internal firewall encloses only a portion of the resources of said personal computer.

77. (Previously Presented) The system of claim 9, wherein said personal computer includes at least one telephone component.

78. (Currently Amended) The system of claim 9, wherein.

at least one server computer is connected to at least one Internet;

at least two personal computers are connected to the server computer through said at least one network;

wherein said server computer is ~~capable of functioning~~ configured to function in a shared processing operation involving said at least two personal computers;

wherein said personal computer is configured to operate with other computers connected to said network utilizing at least one peer to peer wireless network connection ~~capable of directly~~

~~coupling~~ configured to directly couple said personal computer to at least one of said other personal computers via the wireless network connection without connecting to said server computer.

79. (Previously Presented) The system of claim 37, wherein said firewall is configured to protect network use from unauthorized surveillance of at least one said microchip microprocessor processing unit of said at least one personal computer by at least one user of said personal computer during said shared operation.

80. (Previously Presented) The system of claim 37, wherein said firewall is configured to protect network use from intervention in at least one said microchip microprocessor processing unit of said at least one personal computer by at least one user of said personal computer during said shared operation.

81. (Previously Presented) The system of claim 68, wherein said internal firewall is configured to protect network use from unauthorized surveillance of at least one said microchip microprocessor processing unit of said at least one personal computer by at least one user of said personal computer during said shared operation.

82. (Previously Presented) The system of claim 68, wherein said internal firewall is configured to protect network use from intervention in at least one said microchip microprocessor processing unit of said at least one personal computer by at least one user of said personal computer during said shared operation.

83. (Previously Presented) The system of claim 9, wherein said user of said personal computer is an owner of said personal computer.

84. (Previously Presented) The system of claim 42, wherein said user of said personal computer is an owner of said personal computer.

85. (Previously Presented) The system of claim 74, wherein said user of said personal computer is an owner of said personal computer.

86. (Previously Presented) The system of claim 9, wherein said network comprises the Internet and/or an intranet.

87. (Previously Presented) The system of claim 42, wherein said network comprises the Internet and/or an intranet.

88. (Previously Presented) The system of claim 74, wherein said network comprises the Internet and/or an intranet.

89. (Currently Amended) The system of claim 74, wherein said microchip has at least one internal firewall ~~capable of allowing and denying~~ configured to allow and deny access to portions of said microchip both to said user of said server computer and to users from said network and said firewall is a hardware firewall.

90. (Previously Presented) The system of claim 89, wherein:

said internal firewall is further configured to deny access to at least said microchip microprocessor control unit of said server computer by at least one other computer during a shared operation involving said server computer and said at least one other computer of said network; and

said internal firewall is further configured to allow access to at least one said microchip microprocessor processing unit of said server computer by at least one other said computer of said network during said shared operation.

91. (Previously Presented) The system of claim 90, wherein said internal firewall is configured to deny access to at least said microchip microprocessor control unit of said server computer by said other computers of said personal network system during a shared operation involving said server computer and at least one of said other computers of said network.

92. (Previously Presented) The system of claim 91, wherein said internal firewall is configured to allow access to at least one said microchip microprocessor processing unit of said server computer by said other computers of said personal network system during said shared operation.

93. (Previously Presented) The system of claim 92, wherein said internal firewall is configured to deny access to at least one said microchip microprocessor processing unit of said server computer by at least one user of said server computer during said shared operation.

94. (Previously Presented) The system of claim 92, wherein said internal firewall is configured to protect network use from unauthorized surveillance of at least one said microchip microprocessor processing unit of said at least one server computer by at least one user of said server computer during said shared operation.

95. (Previously Presented) The system of claim 92, wherein said internal firewall is configured to protect network use from intervention in at least one said microchip microprocessor processing unit of said at least one server computer by at least one user of said server computer during said shared operation.

96. (Previously Presented) The system of claim 74, wherein said firewall includes hardware or software or firmware or any combination thereof.

97. (Previously Presented) The system of claim 74, wherein said server computer is configured so that at least one user of said server computer retains preemptive control of all components of said personal computer.

98. (New) The system of claim 9, wherein said internal firewall is configured to permanently deny access to portions of said microchip from said network.

99. (New) The system of claim 9, wherein said shared use includes unauthorized shared use, including intrusion by hackers from outside said personal computer.

100. (New) The system of claim 42, wherein said internal firewall is configured to permanently deny access to portions of said microchip from said network.

101. (New) The system of claim 42, wherein said shared use includes unauthorized shared use, including intrusion by hackers from outside said personal computer.

102. (New) The system of claim 74, wherein said internal firewall is configured to permanently deny access to portions of said microchip from said network.

103. (New) The system of claim 74, wherein said shared use includes unauthorized shared use, including intrusion by hackers from outside said personal computer.